USPS Cyber Intrusion and Employee Data Compromise
Updated Dec. 18, 2014
Employee Frequently Asked Questions

1. **How and when did the security breach occur?**
   The Postal Service recently learned of a cyber intrusion into some of its information systems. This type of intrusion is not unique. You likely have read multiple news stories on similar intrusions into U.S. companies and other Federal government agencies. We are not aware of any evidence that any of the compromised employee information has been used to engage in any malicious activity. We are working closely with the Federal Bureau of Investigation, Department of Justice, the USPS Office of Inspector General, the Postal Inspection Service and the U.S. Computer Emergency Readiness Team. The Postal Service has also brought in private sector specialists in forensic investigation and data systems to assist with the investigation and remediation to ensure that we are approaching this event in a comprehensive way, understanding the full implications of the intrusion and putting in place safeguards designed to strengthen our systems.

2. **Why were employees not told of the breach immediately after it was discovered?**
   Communicating the breach would have put the remediation actions in jeopardy. We are unaware of any evidence that any of the compromised employee information has been used to engage in any malicious activity or to enable identity theft crimes.

3. **Which Postal Service employees were impacted by the breach?**
   Files containing personally identifiable information (PII) for all active employees were compromised. Employees affected include the Postmaster General, other members of the Executive Leadership Team, PCES and EAS employees, craft employees and all other employees. It also includes employees who work for the Postal Inspection Service, the USPS Office of Inspector General and the Postal Regulatory Commission. These files may also have included PII for employees who left the organization anytime from May 2012 to the present.

   Update: In addition, as we first reported on Nov. 10, 2014, the intrusion included a possible compromise of injury-claim data. The investigation has provided the Postal Service with additional information about the file containing this data that is shared with the Department of Labor. The investigation indicates that the file that was potentially compromised was created in August 2012 and contains information associated with current and former employee injury compensation claims. The data included in the file dates from November 1980 to August 30, 2012. Individual letters are being sent to those affected providing them with specific information about their particular situation. Those former employees who have not already received

an offer for a credit-monitoring product will receive information on how to enroll in a free one-year monitoring product. Some of these individuals will not receive a notice letter at this time because they were in the group that received the original letter from the Postmaster General offering the free credit monitoring product and no additional personally identifiable information has been identified as being compromised in their cases.

4. **What information was accessed?**
   While the investigation is continuing, we have determined that the information potentially compromised in the incident included some employee personally identifiable information (PII) such as names, dates of birth, Social Security numbers, addresses, beginning and end dates of employment, emergency contact information and other information. For the current and former employees affected by the possible compromised injury claim data, the type of information potentially compromised varies greatly based on the individual cases.

5. **How could the Postal Service let all this employee information get accessed?**
   No company or organization connected to the Internet is immune from the type of malicious cyber activity the Postal Service experienced. We take such threats seriously and regularly take action to protect our networks, our customers' data, and our employees' information. In this case, a sophisticated intruder was able to get around our defensive measures. As a result of this incident, we have significantly strengthened our systems against future cyber intrusions.

6. **Why were Postal Service information networks taken off-line before the breach was announced?**
   To improve the security of our information networks, the Postal Service performed maintenance and upgrades of its computer and information systems during the weekend of Nov. 8-9, 2014, bringing some systems off-line. This process allowed the organization to eliminate certain system vulnerabilities.

7. **What steps can I take to protect myself and avoid becoming a victim?**
   Because of the personal nature of the information involved, here are some steps you should take to protect yourself:
   - Enroll in Equifax Credit Monitoring. The Postal Service is making this product available to all employees at no charge for one year. You have 90 days from the date of a letter you have received from the Postal Service to take advantage of these services. They are designed to help protect you. We encourage you to take advantage of this product. Your unique activation code is at the top of the letter you will receive.

- Keep vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. If you discover any suspicious or unusual activity on your accounts or you suspect fraud, be sure to report it immediately to your financial institutions and to local law enforcement. Additionally, the Federal Trade Commission provides comprehensive information at www.ftc.gov/idtheft, or you can call the FTC's identify theft clearing house at 1-877-438-4338 (TTY: 1-866-653-4261), or write to the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- On an ongoing basis, you should obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting *www.annualcreditreport.com*, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf. You can also purchase a copy of your credit report by contacting one of the three national credit reporting agencies. You may contact the national credit reporting agencies at:
    - Equifax: 1-800-525-6285; or www.equifax.com; or P.O. Box 740241, Atlanta, GA 30374-0241
    - Experian: 1-888-397-3742; or www.experian.com; P.O. Box 9532, Allen, TX 75013-9532
    - TransUnion: 1-800-680-7289; or www.transunion.com; P.O. Box 6790, Fullerton, CA 92834-6790

8. **What if I want to continue to receive credit monitoring from Equifax beyond one year? Can I renew by enrollment or will I have to start the process all over?**
   Equifax will notify employees prior to the end of their free subscription period that their subscription will be expiring. Employees will be given an opportunity to extend the subscription at their expense.

9. **Should I change my ACE ID and password, Postal EIN or other postal passwords as a result of this incident?**
   At this time there is no requirement to change your ACE password or other passwords unless prompted to do so by email prompts from IT as part of the normal password change process. You will be notified if other password changes are required. Your Postal EIN and ACE ID will not be changing as a result of this incident.

10. **How do I know if my banking information was affected by this breach? Should I call my bank and creditors?**
    We are unaware of any evidence that the compromised employee information has been used to engage in malicious activity. Postal Service forensic investigators are conducting a thorough review of the affected databases, and if the ongoing investigation determines that any additional employee information has been compromised, you will be notified. Postal employees, like everyone else, should keep vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or you suspect fraud, be sure to report it immediately to your financial institutions and to local law enforcement. Postal employees, like anyone else, can always contact their bank or other financial institutions to change their account information if they wish to do so.

11. **What precautions have been taken since the breach?**
    Through the investigation we identified the methods and locations that were used to gain access to some of our data systems and devised a plan to close those access routes to prevent future intrusions. We also are instituting numerous additional security measures. Some are equipment and system upgrades that will not be visible to users, and some are changes in policies and procedures that we will be rolling out in the coming days and weeks.

    We are unaware of any evidence that the compromised employee information has been used to engage in malicious activity. Postal Service forensic investigators are conducting a thorough review of the affected databases, and if the ongoing investigation determines that any additional employee information has been compromised, you will be notified. Postal employees, like everyone else, should stay vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or you suspect fraud, be sure to report it immediately to your financial institutions and to local law enforcement. Postal employees, like anyone else, can always contact their bank or other financial institutions to change their account information if they wish to do so.

12. **Why is VPN not working? When will it come back and will there be any changes to it?**
    VPN was identified as vulnerable to this type of intrusion and will remain unavailable as we work to make modifications to this type of remote access to our networks. When VPN is available again users will notice changes in functionality. We will have additional information about VPN in the near future.

13. Will I be held liable for ANY fraudulent activities on my personal information or banking accounts?

By enrolling in the free Equifax Credit Monitoring product, you will receive up to $1 million in identity theft insurance with no deductible and no other cost to you. Again, we are unaware of any evidence that the compromised employee information has been used to engage in malicious activity or to enable identity theft crimes.

14. Have any lessons been learned from this?

The security of our information systems has always been a top priority. Now the Postal Service has joined the growing list of major companies and governmental agencies that have fallen victim to cyber intrusions. Despite this breach, we will continue to make every effort to safeguard employees' personal information. This is a responsibility we continue to take very seriously. The leadership of the Postal Service is committed to taking steps to strengthen the security of our systems and provide you with the resources you need as a result of this incident.

15. I want to speak to someone about these issues. Who should I contact?

Please contact the Postal Service Human Resources Shared Services Center at 1-877-477-3273 and chose option 5 (option 1 for TDD/TTY). You can also discuss this matter with your local human resources representative.

16. Are the services of the Employee Assistance Program available in connection with this incident?

The Postal Service Employee Assistance Program is available to help any employee deal with this issue. Information or assistance is available 24 hours a day, seven days a week. Please call 1-800-EAP-4-YOU (1-800-327-4968) or visit www.eap4you.com.

17. Will all individuals who have left the organization since May 2012 (active and off rolls) be receiving the first letter to their address of record?

The letter was sent to the address of record for anyone who has been an employee at any time since May 2012 (excluding people just hired in October and November).

18. For current employees on active duty military, how will they be notified of the information we will be sharing today?

There are no special arrangements for notice to employees serving on active duty. For anyone who does not or cannot receive the letter, we are relying on the alternative notice that we are providing through the media and our website. This is the normal form of notice in these circumstances for anyone for whom we do not have a current mailing address.

19. Was benefits information compromised (i.e., beneficiaries, health plan, life insurance, etc.)?

We do not believe that any of the information related to benefits was compromised with the exception of the fact than an employee has a benefit, and which benefit he or she chose (i.e., no account number). However, the fact that the employee had, for example, the Blue Cross/Blue Shield Family Plan, is among the data that may have been compromised. (In other words, the basic information on a Form 50, but nothing more regarding benefits.)

20. Are Postal Service affiliated credit unions going to be notified?

No USPS Credit Unions have been affected by this security breach. They have been notified of the breach.

21. How will this impact the Postal Service's bottom line?

As you know, cyber-attacks are a continuing threat to businesses and agencies that maintain data electronically. The Postal Service is not immune to such attacks, as was made evident on Nov. 10 when we announced that we had been victimized by a cyber-security intrusion.

Our operational and administrative information systems are among the largest and most complex systems maintained by any organization in the world. Any disruption, including those impacting computer systems that facilitate mail handling and delivery and customer-utilized websites, could adversely impact customer service, mail volumes and revenues and result in significant increased costs. A significant systems failure also could cause delays in the processing and delivering of mail, or result in an inability to process operational and financial data.

We are working with our external auditors to review our financial applications to confirm that the incident did not compromise financial systems and data. There is no indication at this time that the data was compromised, but out of an abundance of caution, we delayed filing our 10-K — which we had planned to do on November 14 — until the review was completed. The Board of Governors approved the 10-K Dec. 5.

22. Have banking institutions been notified of this cyber intrusion?

Yes

23. How much will the credit monitoring cost the Postal Service?

We can't answer that question until we know how many employees sign up for the product.

24. Will the "free credit monitoring" include a spouse if divorced, and children, as well?

The free credit monitoring product is being offered only to those individuals whose sensitive personal information, such as their Social Security number, was potentially compromised. Although the investigation is ongoing, we do

not believe that any sensitive personal information of family members of employees was potentially compromised.

25. Will emergency contacts have access to the free credit monitoring?
The free credit monitoring product is being offered only to those individuals whose sensitive personal information, such as their Social Security number, was potentially compromised. Although the investigation is ongoing, we do not believe that any sensitive personal information of the emergency contacts was potentially compromised.

26. Who is culpable if fraud activity occurs?
By enrolling in the free Equifax Credit Monitoring product, you will receive up to $1 million in identity theft insurance with no deductible and no other cost to you. Again, we are unaware of any evidence that the compromised employee information has been used to engage in malicious activity or to enable identity theft crimes.

27. Will the Postal Service assume liability for any financial losses that are attributable to this cyber intrusion?
The Postal Service is purchasing the credit monitoring product for all employees whose sensitive personal information was potentially compromised. By enrolling in the free Equifax Credit Monitoring product, you will receive up to $1 million in identity theft insurance with no deductible and no other cost to you. Again, we are unaware of any evidence that the compromised employee information has been used to engage in malicious activity or to enable identity theft crimes.

28. Can you confirm that China was behind the breach?
No. The breach is being investigated and the Postal Service isn't speculating about who is behind it.

29. Has the intruder been identified?
No, the breach is currently under investigation.

30. Has the Inspection Service database of HCR Drivers been compromised?
There is no indication that the contractor database was compromised.

31. What customer data was compromised?
Postal Service transactional revenue systems in Post Offices, as well as on *usps.com* where customers pay for services with credit and debit cards, have not been affected by this incident. There is no evidence that any customer credit card information from postal retail or online purchases such as Click-N-Ship, the Postal Store, PostalOne!, change of address or other services was compromised. The intrusion did compromise call center data submitted by customers who contacted the Postal Service Customer Care Center with an inquiry via telephone or e-mail between Jan.1, 2014, and Aug. 16, 2014. For most of our customers in this group, the ongoing

investigation indicates the file did not include sensitive personally identifiable information. To our knowledge, the data potentially accessed did not include Credit Verification Codes (CVC), Personal Identification Numbers (PIN) or any other payment card information. For those customers who provided their credit card numbers between Jan. 1 and Aug. 16, 2014, the Postal Service will offer the same one-year free credit monitoring product being offered to Postal Service employees and some retirees. This small group of customers (approximately 100) will receive a letter with additional details about the cyber breach and instructions on how to enroll in the free credit-monitoring. At this time, we do not believe that any other customers potentially affected by the incident need to take any action. We are unaware of any evidence that the compromised customer information has been used to engage in malicious activity or to enable identity theft crimes.

32. Have the Thrift Savings Plan accounts for Postal Service employees been compromised?

No. TSP is hosted by the TSP system. This incident does not affect your Thrift Savings Plan account. As a reminder, you can always visit the TSP Security Center for information regarding online security.

33. Have our travel/purchasing cards been compromised?

No. No travel/purchasing cards have been compromised in this security breach.

34. Were contract employees' information compromised? If so, will they be receiving free credit monitoring and a letter?

No. Contract employee information was not compromised during this security breach.

35. Has any information in the eOPF been compromised?

No. The eOPF system was not compromised during this security breach.

36. Employees on long-term leave are off-site and unable to access or view USPS communications, including email. How will these employees be informed of what is happening?

All affected employees will be receiving a letter mailed to their address of record containing all relevant information pertaining to this security breach.

37. Are we monitoring changes being made on PostalEASE?

No. The interactive Voice Response (IVR) has been turned off and we enhanced the security of the password reset function. Employees should make sure they update their Self service profile (SSP) password.

38. When will telecommuting be restored?

When the proper security processes and administrative/management practices are implemented. You will be notified when the telecommuting program is approved to resume.

39. Was the Social Security Information (SSI) of the emergency contact listed also compromised?
No. The Social Security information of the emergency contact listed was not compromised.

40. Will employees receive new uniform bank cards as a result of the cyber intrusion?
No. No USPS Uniform bank cards were compromised during this security breach.

41. Was the information of applicants compromised and does messaging need to be sent to them?
eCareer was not compromised during this security breach.

42. What data systems were turned off and will not be restored?
Advance and ePubWatch are applications that will not be restored.

43. How will we know if our personal accounts/personal email accounts have been accessed by unauthorized persons?
We cannot tell if your personal email account has been accessed. We are encouraging all employees to take steps to safeguard against any potential abuse of their personal information. For instance, employees should stay vigilant for incidents of fraud and identity theft by regularly reviewing their account statements and monitoring their credit reports.

44. Our Detached Mail Units operate off the VPN network. Has anyone discussed what will be the impact to this operation relating to mail acceptance and verification, and even more importantly, financial fund transfers to and from customer accounts that take place using the Postal CAPS system?
There are a total of 416 DMU locations impacted by a lack of connectivity due to the VPN network being down. Acceptance employees have been following contingency processes to ensure customer operations are not impacted and postage is collected. Mailings and associated postage statements are still being accepted at the DMU locations. At the end of the tour, hardcopy postage statements are brought to the associated BMEU to be entered into PostalOne! and electronic postage statements are accessed through PostalOne! at the associated BMEU and billed each day. There should be no impact to customer CAPS or advanced deposit accounts.

45. Is the unavailability of Office Messenger at Headquarters this week related to the cyber intrusion?
No. This service is not operating due to technical reasons not related to the cyber intrusion.

46. Is there any impact to weekly payroll?
No. There is no impact to the weekly payroll.

47. Will the Postal Service pay for freezing and thawing of Social Security numbers?

Social Security numbers cannot be frozen or thawed.

48. If an employee or retiree has died since May 2012, is the surviving spouse eligible for the free credit monitoring? If so, would that be in the employee's name only or in the name of the estate and/or surviving spouse?

No, a surviving spouse is not eligible for free credit monitoring because the surviving spouse's information was not compromised. If the person entitled to credit monitoring is deceased, Equifax recommends that the spouse, attorney, executor or administrator of the deceased person's estate mail a copy of the death certificate to each company at the addresses below. Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven-year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response to the spouse, attorney, or executor of the estate. The other two companies may have different procedures upon receipt of the death certificate.

Equifax:	Experian:	Trans Union:
Equifax Information Services LLC Office of Consumer Affairs P.O. Box 105169, Atlanta, GA 30348	Experian Information Services P.O. Box 9530 Allen, TX 75013	Trans Union Information Services P.O. Box 1000 Chester, PA 19022

49. Was any data compromised from customers who use the Secure Destruction system?

No, there is no known impact from the breach on Secure Destruction customers.

50. Why is the Postal Service still using our Social Security numbers when employees were asked to convert to Employee Identification Numbers several years ago?

The Postal Service has converted its internal systems to using Employee Identification Numbers (EIN). However, the Social Security number is collected for the purposes of reporting to other agencies such as the Social Security Administration, Internal Revenue Agency and the Office of Personnel Management.